Chapter 4

Information Assurance and Protection

The Army relies on information to plan operations, deploy forces, and execute missions. Information and telecommunication systems provide the distribution of information that enhances our warfighting capabilities. Increasing reliance on these system technologies makes these systems more likely to experience attacks, intrusions, and interruptions. This chapter discusses the threat to our national information and communications infrastructure and the roles and responsibilities of the agencies and personnel involved in IA and protection as functions and tasks of NSM.

THREAT

4-1. Threats to our national information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing. They come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, personal, or industrial gain.

4-2. Perpetrators have different motives for penetrating computers, networks, and systems. Some perpetrators look for amusement; they break in to obtain interesting data for the challenge of using someone else's computers or to compete with other hackers. Although curious, they are not actively malicious, though at times they inadvertently cause damage to these systems. Computer vandals or attackers, however, deliberately set out to cause harm to particular organizations, and in doing so, attempt to ensure their adversary knows about the attack. Some intruders are professional thieves and spies who aim to break in, copy data, and leave without notice or damage. Often, because of the sophistication of the tools they use, their attacks go undetected. The DOD infrastructure is especially attractive because it develops and works with advanced research data and other information interesting to foreign adversaries, commercial competitors, and other curious people.

4-3. The globalization of network communications creates vulnerabilities due to increased access to the information infrastructure from points around the world. Threats against computers, BISs, AISs, networks, and systems vary by the level of hostility (peacetime, conflict, or war), technical capabilities, and motivation of the perpetrator. Threats to strategic and tactical forces exist from a variety of new and different sources, and they exist on a continuing basis even during periods of relative peace.

4-4. Attacks and intrusions compromise missions, degrade network and systems, and in some cases, destroy hardware and software applications.

This hampers the effectiveness of support forces and the supported warfighter.

4-5. It is virtually impossible to defend against all the vulnerabilities our information infrastructure and information processes may experience. However, IA and protection programs ensure that the necessary protection and defense mechanisms are in place to help protect against these vulnerabilities.

CATEGORIES

4-6. Threat generally falls into three categories: intentional, unintentional, and environmental.

Intentional

4-7. An intentional intrusion into network and systems is a deliberate act. These acts, considered criminal in most cases, have proven to be one of the most challenging to protect, detect, and react against.

4-8. **Unauthorized Users**. Unauthorized users, such as hackers, are the source of most attacks against information systems (INFOSYS) in peacetime. They mostly target personal computers, but recently have targeted network communications, mainframes, and netted computers.

4-9. **Trusted Insiders.** Individuals with legitimate access to a system pose one of the most difficult threats to defend. Whether recruited or self-motivated, insiders have access to systems normally protected against attack. While insiders can attack a system at almost any time, a system is most vulnerable at design, production, transport, and maintenance.

4-10. **Terrorists.** Terrorists are increasing their use of commercial INFOSYS (including the Internet). They may obtain unauthorized access to an information network or direct attacks against the infrastructure (bombing). Terrorist groups use computer bulletin boards and Internet and Intranet systems to pass intelligence and technical data across international borders. These organized groups pose a serious threat to our information infrastructure and national security.

4-11. **Nonstate Groups**. Drug cartels and social activists take advantage of the possibilities offered by the Information Age. They can acquire at low cost the capabilities to strike at their foes' commercial, security, and communications infrastructures. Moreover, they can strike at a distance with little impunity. In addition to attacking opponents directly, nonstate groups use the international news media to influence global public opinion and shape perceptions of a conflict or differences in governments. They even attempt to inflame dormant issues into conflicts that otherwise would not arise.

4-12. **Foreign Intelligence Services.** Foreign intelligence services are active during peace and conflict and take advantage of the anonymity offered by the computer, bulletin boards, and the Internet. They hide organized collection or disruption activities behind the facade of unorganized hackers. Their primary targets are often commercial, scientific, and university networks, as well as direct attacks on military and government networks and systems.

4-13. **Opposing Militaries or Political Opponents.** While the adversary's activities are more traditionally associated with open conflict or war, opposing militaries or political opponents may invade our computer and telecommunications networks during peacetime. This helps frame the situation to their advantage preceding the onset of any hostilities. Adversaries may try to manipulate the news media and public opinion to their advantage.

Unintentional

4-14. The unintentional intrusion into networks, systems, and computers occurs more often than realized. In many cases, the intruder does not realize they entered a restricted network, device, or system. The unintentional category covers other areas of mistakes and mishaps and is nonspecific.

4-15. **Insider Misuse**. Network and systems misuse is a problem and concern for all government agencies and private industries. Insiders of these organizations tie up networks and systems by sending chain letters, frivolous e-mails, and jokes; listening to broadcasts via the Internet; and other unauthorized uses.

4-16. **Clumsiness**. Clumsiness of operators and network managers can bring havoc to a network. This normally happens when a command or action code erroneously inserted into the network or system activates and becomes a real-time action. These mistakes take place during network planning or the operational stage. Other events, such as cable cuts, may also bring havoc to networks and systems.

4-17. **Contamination**. Software applications and equipment hardware contamination occur in the development, manufacturing, and upgrading stages of the product. This is different from the intentional development and distribution of viruses or logic bombs. Though unintentional, it brings misfortune and proves to be very costly for government, industry, and individuals.

Environmental

4-18. Lightning strikes, electromagnetic interference, high winds, tornadoes, and rain pose a threat by corrupting data, physically destroying equipment and property, and causing denial of service threats. In addition, power outages pose a denial of service threat similar to a physical attack.

ATTACKS

4-19. Some attacks against INFOSYS, computers, networks, and systems have a delayed effect and others are immediate. Both of these attacks corrupt databases or controlling programs and may degrade or physically destroy the INFOSYS. Below is a description of the different types of attacks. For more detailed information on attacks, refer to the related Defense Intelligence Agency-approved documents.

Computer

4-20. Computer attacks generally aim at software or data contained in either end-user or network infrastructure computers. Adversaries aim at unauthorized but unobtrusive access to information, unauthorized modification to software and/or data, or total destruction of software and data. These activities can target individual computers or large numbers of computers connected to a LAN or WAN.

4-21. Computer attacks may take place during routine tactical operations and may be multifaceted to disrupt major military missions. They can be part of a major nation-state effort to cripple the US national information infrastructure. Adversaries conduct computer attacks during wartime and peacetime. These threats include incompetent, mischievous, or vengeful insiders; criminals; political dissidents; terrorists; and foreign espionage agents. Computer attacks may involve unauthorized copying of files, direct deletion of files, or introduction of malicious software or data. Malicious software is generally executable software code secretly introduced into a computer and includes viruses, Trojan horses, trap doors, and worms. Malicious data insertion, sometimes termed spoofing, misleads a user or disrupts system operation. For example, an attack disrupts a packet data network by introducing false routing table data into one or more routers. An attacker who is otherwise not able to deny service or corrupt data on a wide scale may weaken user confidence in the information they receive by corrupting or sending false data.

Physical

4-22. Physical attacks generally deny service and involve destruction, damage, overrun, or capture of the system components. This may include end-user computers, communications devices, and network infrastructure components. Physical attacks involving overrun and capture allows the adversary to employ a computer attack. These attacks may be–

- Sabotage.
- Small arms.
- Automatic weapons.
- Tanks.
- Guided/unguided missiles.
- Tube artillery.
- Bombs.
- Munitions ranging from dumb bullets to “brilliant” sub-munitions.

Theft

4-23. Theft is a physical attack that does not involve destruction/damage. Theft of items such as cryptographic keys and/or passwords is a major concern since these items can be used to support subsequent electronic or computer attacks.

Electronic

4-24. Electronic attacks focus on specific or multiple targets within a wide area. Attacks against communications links include two types of signal intelligence (SIGINT) operations: signal intercept and analysis to effect compromise of data and emitter direction finding and geo-location to support signal analysis and physical attack. Jamming is another attack against communications links. This corrupts data and may cause denial of service to users. For example, the jamming of communications links supporting Global Positioning System (GPS) users is a specific digitization concern.

High Energy

4-25. High-energy attacks are generally denial of service attacks that purposely destroy or damage their targets. Electromagnetic pulse (EMP) generators that destroy or damage electronic devices are a main concern. This includes medical, vehicular, aircraft, and communications equipment. The adversary's ultimate goal is to overload components with induced and direct energy weapons.

PRINCIPLES

4-26. Commanders develop comprehensive protection programs in anticipation of how an adversary may employ elements of attack and intrusions that disrupt C2 systems and decision-making processes. IA and protection principles are to–

- Gain C2 superiority. This includes the unimpeded friendly processing of information, accurate development of courses of action (protect, detect, and react), valid decision making, efficient communications to and from subordinates, and training in IA and protection.
- Remain inside the adversary's decision cycle by denying, influencing, degrading, and/or destroying the adversary's C2, personnel, equipment, telecommunications, and AISs.
- Reduce the adversary's capability to conduct attacks and intrusions.
- Reduce friendly vulnerabilities by using protective measures. For example, hardening information systems with protection devices and techniques to deter attacks and intrusions.
- Reduce friendly and foe interference in our networks and systems throughout all levels of NSM.

ROLES AND RESPONSIBILITIES

4-27. All network and systems users are responsible for the security of the devices they use. AR 380-19 describes the ISS program and the authority of protecting these systems. This regulation requires structured ISS, security personnel, and procedures to combat intrusions into networks and systems. Specific organizations and personnel within the Army respond to intrusions and attacks of networks and systems. They work closely together to prevent, detect, and react to intrusion and attacks to our information infrastructure. The paragraphs below discuss the roles and responsibilities of some of the organizations and personnel that deal with IA and protection.

DISA

4-28. DISA provides IA and protection programs and structures for the DII. It provides the automated system security incident support team (ASSIST) and closely works with various response teams and organizations to combat the threat. Refer to the ASSIST web page at http://www.assist.mil for more information.

LIWA AND CERT

4-29. The ACERT program consists of a central coordination center and RCERTs under the land information warfare activity (LIWA). The RCERTs and LCERTs perform the operational CERT mission, and the ACERT coordination center provides the coordination and funding for the program. The commander, network manager, or user notifies the local ISSO when an actual or potential security incident or intrusion is detected. The ISSO then reports the incident or intrusion to the supporting CERT/TNSOC activity. The CERT works with the network manager and customer to identify the problem, remove the threat, and recover from the incident. These teams respond to incident reports and coordinate actions IAW CJCSI 6510.01B, appropriate service regulations, and public laws governing such activity.

4-30. Reporting procedures for incidents of intrusion and attacks flow vertically and horizontally to all levels of chain of command, ISSO, CERT, ANSOC, and ASSIST activities. This allows notification and area view by authorized organizations to combat an all out attack against networks, systems, computers, and the DII.

4-31. The ANSOC and TNSOC organizations assist in the war against hackers, intrusions, and viruses and assist with other technical assistance, when needed. The ANSOC, TNSOCs, ACERT, RCERT, and some LCERTs can enter local PCs, LANs, or WANs by using specific management tools. The standard doctrine for this action is that these organizations will assist and enter networks, equipment, and systems only when requested and invited by commanders, network managers, or system administrators of the said equipment. As the primary network managers, the ANSOC and TNSOC do not require any specific permission to protect, deter, or react to attacks or intrusions of networks or systems that they are responsible for managing. These organizations perform their duties IAW AR 380-19, AR 380-53, and other pertinent SOPs and public laws governing their activities. Figure 4-1 shows the infrastructure of the organizational CONOP.

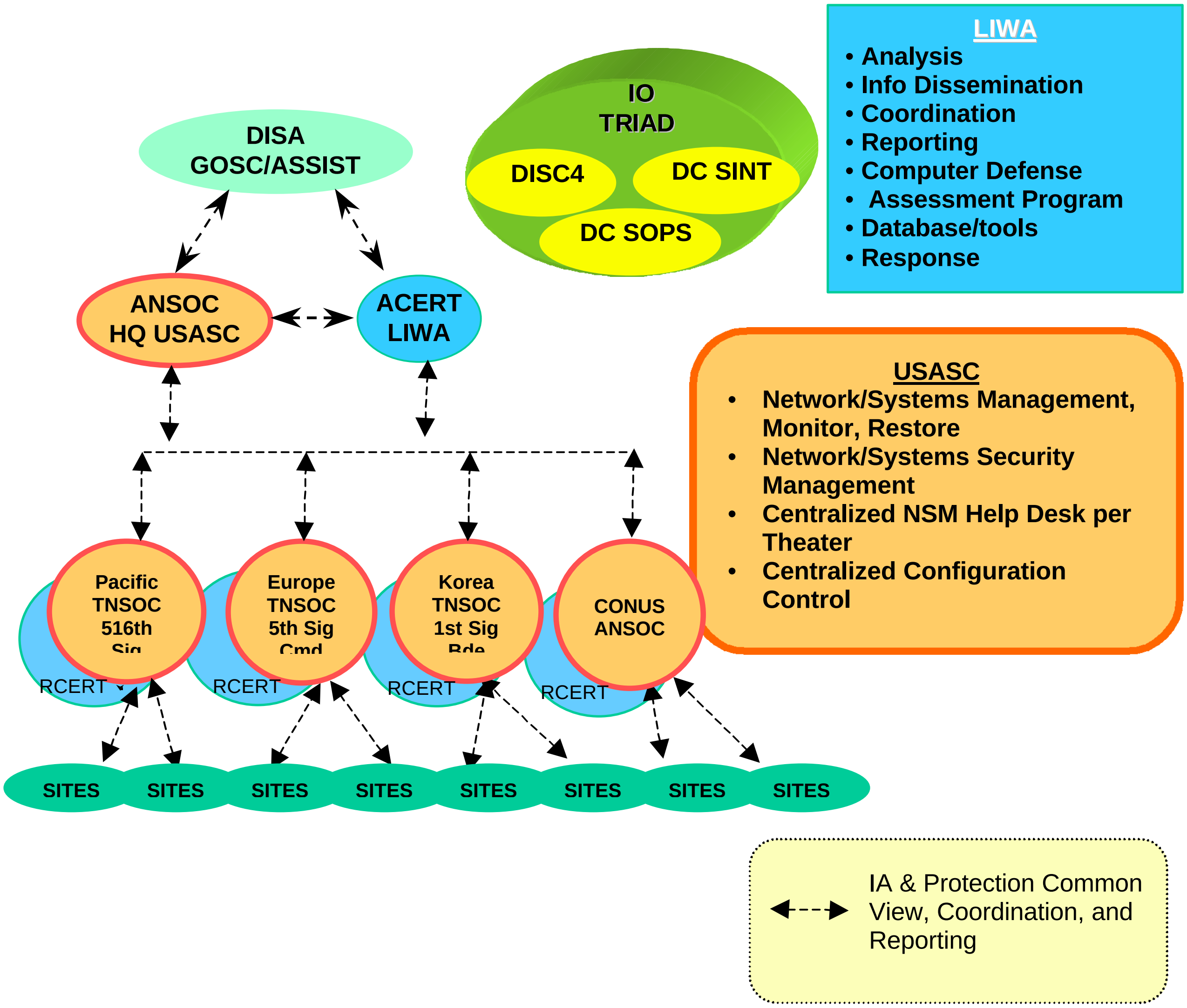

Figure 4-1. ACERT/RCERT Infrastructure Organizational Concept of Operation

INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM)

4-32. An ISSPM is appointed at each Army MACOM and within the Office of the Administrative Assistant to the Secretary of the Army, Program Executive Office, Command, Control, and Communications Systems Force Integration Office (PEOC3S FIO). The ISSPM establishes, manages, and assesses the effectiveness of the ISS program at his command or activity. The ISSPM has personnel assets that manage the computer security (COMPUSEC) and COMSEC subdisciplines of ISS. See AR 380-19 for further information systems security details.

4-33. The ISSPM–

- Appoints an information systems security manager (ISSM).
- Develops security architecture.
- Coordinates and reviews operational concepts, SOPs, and security accreditation for C2 systems.
- Ensures certifications of individual systems are completed.
- Ensures transient electro-magnetic pulse emanation suppression (TEMPEST) certifications of individual systems are in IAW AR 381-14.

INFORMATION SYSTEMS SECURITY MANAGER

4-34. An ISSM is appointed at levels of command below Army MACOM, at the PEO level, and at DA staff and field operating agencies. The ISSM establishes and implements an ISS program for all AISs and AISs under development. This includes posts, installations, and installation equivalents. The ISSM–

- Develops system operational concepts, security SOPs, and security accreditation. Accreditation requests require ISSPM review and are then sent to the designated accreditation authority (DAA) for further action.
- Conducts individual systems risk assessment for operation of unit's systems.
- Conducts system-specific security training and awareness programs.

DESIGNATED ACCREDITATION AUTHORITY

4-35. A DAA is responsible for the overall security of each AIS. Before operation, the DAA certifies each AIS and approves the accreditation IAW approved security requirements and safeguards. See AR 380-19 for DAA policy, responsibility, and procedures.

INTELLIGENCE OFFICER (S2)

4-36. The S2 identifies and assesses foreign intelligence threats to command assets. The S2–

- Administers the personnel security program.
- Ensures the command statement of intelligence interest (SII)(AR 381-19) registers requirements for receipt of validated intelligence affecting the integrity and reliability of the network.
- Provides assistance identifying threat factors for risk management of threats and implements security safeguards.
- Provides gateways to national intelligence agencies for commanders and managers to request information to fill intelligence gaps developed during any phase of the network security process. Specifically, the S2 evaluates security incidents and implements reporting procedures.

G6/S6/S3

4-37. The G6/S6/S3 has overall responsibility for secure operation; therefore, the G6/S6/S3 has management oversight over the ISSO.

Information System Security Officer

4-38. The automation officer, systems integration technician, or systems administrator normally serves as the ISSO. The ISSO–

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for C2 systems security.
- Prepares or oversees the certification and accreditation documentation of systems IAW AR 380-19.
- Coordinates with the brigade S2 to ensure users have the required security investigations, clearances, authorizations, and need-to-know.
- Establishes and implements a system for issuing, protecting, and changing system passwords.
- Establishes the training and awareness programs.
- Manages the interconnection of systems to the network and monitors, reviews, and evaluates the security impact of changes.
- Assesses direct threat and vulnerability, enabling the commander to analyze the risks to the ABCS and interconnected systems.
- Determines appropriate measures to manage network risks effectively.
- Oversees the review of network and system audit trails, resolves discrepancies, and reports incidents to the brigade S2 for evaluation and reporting.

USER

4-39. Each systems operator and user is responsible for security. The operator/user–

- Secures operations of his systems.
- Ensures his terminal is operated properly according to procedures and SOP; performs other duties as assigned by the ISSO and network manager to ensure security and protection of the network and system.
- Follows regulatory and policy restrictions for authorized use of government computers.

SHARED AREA OF RESPONSIBILITY

4-40. IA and protection maintains effective C2 of forces by leveraging advantages provided by digitization and negating adversary that influence, degrade, or destroy C2 systems. The goal of IA and protection is to integrate signal operations, technical engineering, security disciplines, and intelligence (or counter-intelligence) support to ensure the availability, integrity, and confidentiality of information. IA and protection shared AORs include protection, detection, and reaction measures. Figure 4-2 shows these shared AORs.

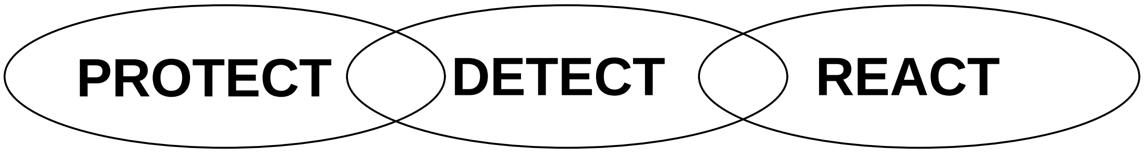

Figure 4-2. Shared AOR

PROTECT

4-41. The Presidential Decision Directive 63 (PDD 63) gives primary orders and directions for enhancing the network and systems security posture of our nations civilian information structure and DII. Each service and department further defines the PDD 63.

4-42. To carry out orders and directives, each service must devise plans to achieve our IA and protection goals. Figure 4-3 shows an example of network and systems protection. An external digital perimeter consists of COMSEC, router filtering/access control lists, security guards, and, where necessary, physical isolation serving as a barrier to outside networks such as the NIPRNET. Internal digital perimeters consist of firewalls and/or router filtering that serve as barriers between echelons and/or functional communities. Internal barriers of COMSEC and physical security are also required. Local workstation security consists of individual access controls, configuration audit capability, protection and intrusion detection tools, and security procedures.

4-43. Information protection is critical to the military's ability to conduct operations and is the responsibility of leaders, information producers, processors, and users. Information protection applies to any medium and form including hard copy (message, letter, and fax), electronic, magnetic, video, imagery, voice, telegraph, computer, and human. Information protection ensures availability, integrity, authenticity, confidentiality, and validity of information.

4-44. The information protection process involves determining the scope of protection based on the value of information protected and the standards for protecting the information. The protection process should reflect the changing value of information during each operational phase.

4-45. NSM operation centers (such as USASC, ANSOC, and TNSOC) provide near-real time surveillance for network and systems suspicious security events and initiate initial defensive actions to block or contain the attack to minimize the operational impact. Robust and resilient infrastructure architecture contains damage from attacks and makes these systems readily repairable in case of attack. The fundamental criteria are that no single attack leads to failure of a critical function, and no single protection mechanism protects critical functions or systems.

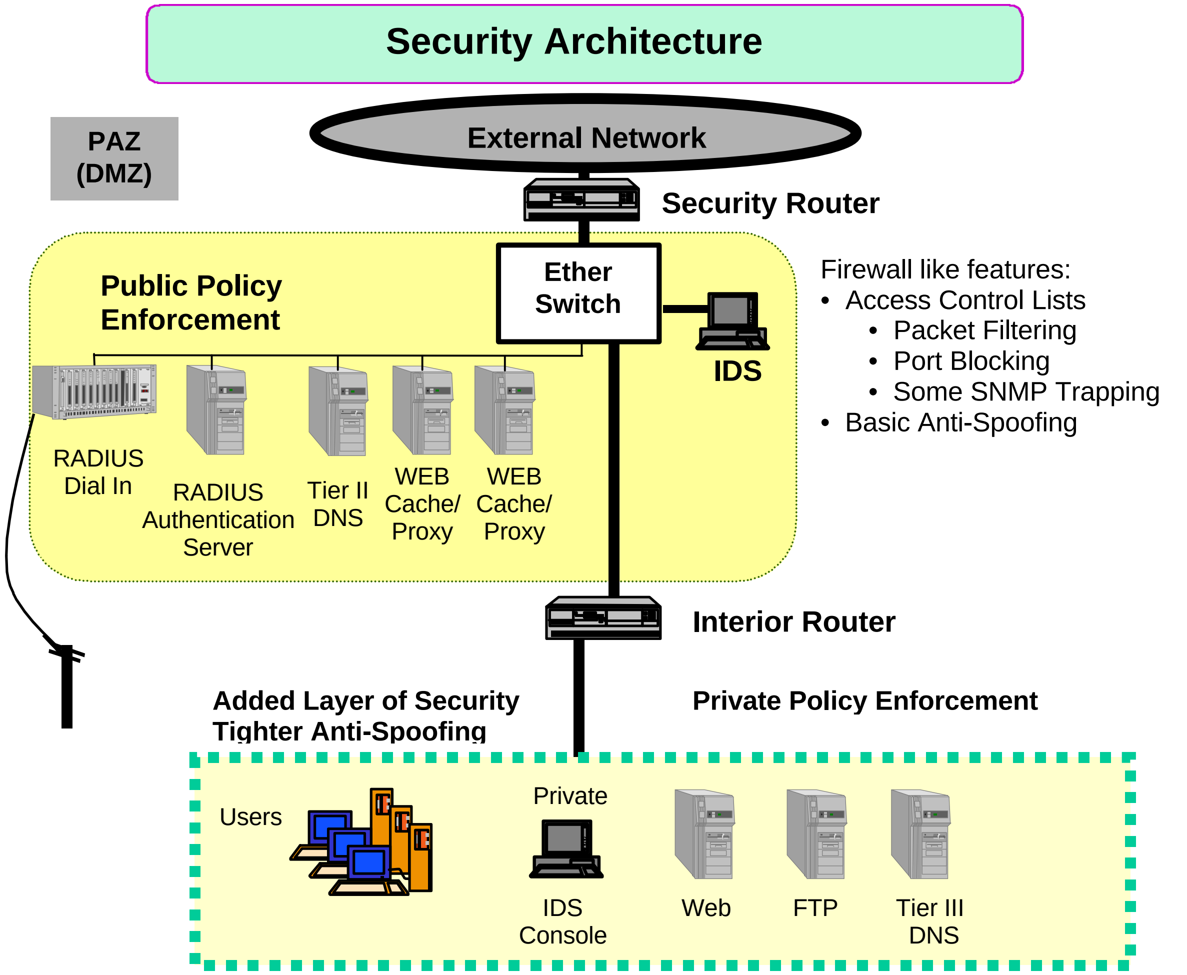

Figure 4-3. Network Infrastructure Protection

4-46. Factors that all users must realize when dealing with IA and protection issues include–

- Comprehensive training programs designed to instill IA, protection, intrusion, and detection doctrine, and operational procedures in all members of the command are required because inadequately trained troops constitute vulnerabilities.
- Vigorous programs for sharing results of red team and vulnerability assessments must be standard practice.
- Intrusion protection and detection systems are necessary.
- Training to protect, detect, and react to intrusions becomes a common task.

4-47. ISS only occurs when a common set of prescribed procedural and technical controls apply to all assets connected to the common user LAN and throughout the WAN. Protection from intrusions into or via a WAN must begin with a cooperative ISS effort between all of the services and the DISA.

4-48. Protection against intrusion into friendly computer networks by denying unauthorized entry and access into these systems is essential for network protection. The vast percentage of intrusions results from human error. Training and operations security (OPSEC) compliance by system managers, operators, and users are the best measures to combat system compromises.

4-49. Network and system managers and administrators must be able to protect against, and prevent intrusions within, their specific AOR by using authorized tools and performing specific tasks as legally authorized by regulations and public law.

4-50. System programs should be hardened against intruders' attempts to gain vital information or damage information flow. No protection plan is perfect, and protection/restoration resources are limited. Operations plans (OPLANs) and operations orders (OPORDs) specify the priorities of protection efforts. Firewalls and intrusion detection software are examples of hardened systems.

4-51. Information provided on the Army's web pages is of particular concern for security purposes. The OPSEC guidelines for web pages are the same as any other information. For specific guidelines on administration policies and procedures, refer to http://www.acert.belvoir.army.mil/frames.html. OPSEC allows the commander to identify actions that adversary intelligence systems and intruders observe. It provides an awareness of the potentially friendly indicators that adversary intelligence systems might obtain. OPSEC identifies, selects, and eliminates (or reduces to an acceptable level) information that is subject to exploitation by adversaries.

4-52. OPSEC planning challenged by new global commercial capabilities, including imaging, positioning, and cellular systems, offers potential adversaries access to an unprecedented level of information against friendly forces. The news media and e-mail users complicate OPSEC during military operations. The ability of the media and others to transmit real-time information to a worldwide audience could be a lucrative source of information to an adversary. OPSEC planners, working closely with Public Affairs (PA) personnel, commanders, and security managers, must develop the essential elements of friendly information (EEFI) used to preclude inadvertent public disclosure of critical or sensitive information.

4-53. Many different measures affect OPSEC. These include counterintelligence, INFOSEC, transmission security (TRANSEC), COMSEC, and signal security (SIGSEC). As more of the Armed Forces transition to networked communications, INFOSEC takes on an ever-growing importance.

4-54. INFOSEC and ISS are critical to INFOSYS within the Army. In war and peace, computer systems and networks on which units rely for logistics, personnel, administration, maintenance, and financial data processing and transfer are vulnerable to attack. Often, the Internet is a favorite communication platform for intruders. Gaining access to a unit's computers and communications networks are accomplished by a wide range of methods and techniques. Some of the more common methods include–

- Inserting malicious software through contractors.
- Tracking software maintenance changes and system operations activities.
- Alternating access paths or sniffer devices that trap information about traffic and passwords.

4-55. These intrusions may initiate during peacetime or at any point in an operation. A military system could come from the factory with embedded viruses or logic bombs. In the past, new commercial floppy disks used by government agencies have contained viruses upon delivery from the factory.

4-56. Accordingly, security measures and procedures must actively and passively preserve the confidentiality, integrity, and functionality of INFOSYS. Protection requirements include near-real-time measures that detect intrusions and alterations, then react and counteract by restoring the INFOSYS needed by commanders to support the military operation. A series of security measures and protection efforts ensure ISS. Security measures that assist in protection are–

- Procedures for quality assurance in all program and hardware acquisition.
- Denial of unauthorized access.
- Hardening of programs and gateways.

4-57. The successful conduct of operations in the information age requires access to information available outside the operational area. Information infrastructures (including critical infrastructures) no longer parallel traditional command lines and warfighters need frequent, instant, and reliable access to information at locations in the CONUS as well as in OCONUS theater. For example, mobility and sustainment of forces are highly dependent on commercial reach-back infrastructures that include international telecommunications, the public switched network, transportation systems, and commercial electric power grids. Our armed forces require secure VTC, database connectivity, and broadcast/receive capabilities for reachback access to intelligence, logistics, and other essential support data.

4-58. The technical complexity of information infrastructures may inhibit a commander's ability to manage the information available to him. Additionally, the availability of information dissemination devices (such as e-mail) may also prove to be a menace when it comes to the security of information that originates from the battlefield.

4-59. Supporting crises and contingency operations require the rapid expansion of C4 capabilities beyond their normal peacetime limits. Our forces must have assurance that this expanded C4 infrastructure can attain the level of protection required to assure mission success. The implementation of this or any other level of protection for the DII requires the cooperative efforts of service providers, the DOD, and government.

4-60. Our dependence on information and information systems and the exposure of our vulnerabilities have brought focus and compelling relevance to the emerging discipline of defensive information operations (IOs). Its unique characteristics set in motion revolutionary capabilities that will enhance and support warfighting into the next century. Defensive IOs occur within the context of four interrelated processes: information environment protections, attack detection, capability restoration, and attack response.

4-61. Relatively few rules and laws govern the use of, or access to, numerous INFOSYS or technologies in the CONUS and OCONUS. Thus, IOs confront legal challenges, interpretations, and other constraints such as rules of engagement (ROE), status of force agreements (SOFA), and status of mission agreements (SOMA). Tension exists both in peace and during times of conflict. Policy and/or law often limit collection of intelligence or simple information in peacetime. Many policies and laws are yet to be determined for using nonmilitary computer systems and other information networks during peacetime.

4-62. Network managers must be aware of regulations, statutes, and public law that govern privacy and monitor activities. The government currently does not advise control or regulation of Internet access that protects sensitive information or critical network nodes. Several initiatives addressing these areas are underway, including PDD 63. Close coordination with the supporting judge advocate is critical in confronting IO challenges at each level of NSM. Counter attack actions are a great legal concern because most are illegal under present federal and state laws and statutes.

4-63. Because many of the actors and influences in the military information environment (MIE) are outside friendly military control, contracts or legal restrictions may prevent the military from controlling or influencing an adversary from using civilian assets. During hostilities, an allied coalition force may depend upon an international agency to change the access codes for an imagery satellite to protect critical information in the AOR. Without the change, the imagery is available in the open market. Thus, it allows downloading of critical satellite imagery of the geographic region in near-real time as the satellite passes over the ground station.

4-64. TRANSEC is an important factor that helps secure information across the various networks. Truck encryption devices, in-line encryption devices, frequency hopping, and time division techniques usually secure transmissions. TRANSEC, using one or more of the techniques and devices listed above, is essential in ensuring INFOSEC.

4-65. COMSEC in networks is an absolute must. Specific keys enable secure encryption of the voice and data passed through transmission devices and computers. The NSA controls most encryption keys and governs local key generation, distribution, and storage of these materials.

4-66. In a private industry-sponsored demonstration, computer enthusiasts used a PC to decode encryption keys that are used for securing banking industry communications. This project was successful in 56 hours and demonstrated how vulnerable voice and data networks are to any individual or adversary with the help of ordinary computer technology. The demonstration also dictated the need for PDD 63. The civilian sector and numerous other government agencies are subject to intrusions and attacks.

4-67. The Force Integration Office (FIO) uses NSM security tools to identify individual system vulnerabilities and apply countermeasures before fielding these systems. They provide configuration parameters and IA and protection NSM guidelines so network managers can maintain configuration control within deployed networks. All BISs must operate in secret systems-high mode to ensure prevention of intrusion into AISs. Any nonsecure system or device connected to or entering any network of secure nature must have an in-line encryption device in use between the network entry point and the entering equipment. This ensures all network security.

DETECT

4-68. NSM facilities can detect occurrences that constitute violation of security policies. Selected events or occurrences (such as numerous log-on attempts within a specified period) are monitored using conventional protection and detection tools. Violations of security policies include–

- **Integrity violation.** An indication that a potential interruption in information flow has occurred, such as information illegally modified, inserted, or deleted.
- **Operational violation**. An indication a requested service is unavailable or has malfunctioned or invocation of service.

4-69. System operators, administrators, and users must train in all aspects of ISS on the BIS or AIS they are required to operate and maintain. They must maintain the BIS and AIS audit functions, review audit information for detection of possible system abuse, and coordinate with the ISSO.

4-70. Appropriate safeguards detect and minimize unauthorized access and inadvertent, malicious or non-malicious, modification or destruction of data. Appropriate safeguards ensure security classification labels remain with data transmitted via a network to another AIS.

4-71. Computer systems are vulnerable to attack when–

- Inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords.
- Weak passwords can easily be guessed.
- Identified security weaknesses go uncorrected.

4-72. Malicious threats can be intentionally designed to unleash computer viruses, trigger future attacks, or install software programs that compromise or damage information and systems.

4-73. Although manufactures design systems with security in mind and personnel follow appropriate procedures, real-time security management and intrusion detection should be a part of routine operations. Appropriate reactive measures must be taken when problems occur. The information systems protection concept envisions real-time security management as a component of, and incorporated into, NSM.

4-74. Security management alerts the network and system manager to intrusion attempts and a range of response mechanisms. Security management–

- Changes boundaries/perimeters.
- Reconfigures firewalls, guards, and routers.
- Reroutes traffic.
- Changes encryption levels or re-keys.
- Zeroizes communications suspected of being compromised.
- Reestablishes a net without selected members.
- Changes passwords and authentication.

REACT

4-75. The Army requires the ability to protect computer systems and data networks and the information they pass and store; detect when an intrusion happens; react to fix the problem; and provide relevant information for IOs. This includes operating during periods of degradation due to operations and hostile attacks and operating with failed components. This requirement derives from the IA and protection program to protect computer systems, networks, and information within the Army.

4-76. Certain security-relevant events alert operators/managers to an intrusion. Security alarm categories are either integrity or operation violations. For security measures, a user must take the following emergency steps–

1. Report the incident to his immediate supervisor, commander, and ISSO.
2. Follow incident security network policy as outlined in the SOP and other applicable regulations.
3. Restore any destroyed/compromised data from backups and CONOP capabilities.
4. Report the incident to other reporting facilities, as required.

TOOLS

4-77. A variety of software and hardware tools enable network managers and security managers to prevent, detect, monitor, and evaluate intrusions into our networks. These tools continuously change as technology changes, and must be an approved tool for use in the networks. The current list of tools is available through the Office, Director of Information Systems for Command, Control, Communications, and Computers (ODISC4) and is distributed to subordinate activities, as necessary. See the G6/S6/ISSO representative for the latest intrusion and protection tools.

4-78. Protection and detection tools–

- Audit monitoring and intrusion detection systems.
- Isolate systems under attack by automated infrastructure management.
- Detect malicious code and eradicate systems.
- Analyze and assess vulnerability.

4-79. These hardware and software tools protect against external and internal hackers and virus attacks. These tools include–

- Anti-virus software.
- Hard-disk purge capability.
- Network mapping software.
- Audit profile software.
- Intrusion detection systems.
- Secure password generation systems.
- In-line network encryption devices.
- Firewalls, high-assurance guards, and tactical security guards.
- Encryption key management systems.
- Security posture of systems and networks.

INCIDENT AND VULNERABILITY REPORTING

4-80. The incident and vulnerability reporting requirements are relevant to all government activities and agencies. Refer to the DOD-ASSIST/CERT web page at http://www.assist.mil/ for DOD service reporting guidelines and procedures. Table 4-1 shows some incident reporting procedures. See CJCSI 6510.01B CH-1 for detailed information on incident and vulnerability reporting.

4-81. Detection of security incidents may cause–

- **Logging.** Recording security-relevant information to facilitate detection and investigation of security breaches, when required. All devices require reporting to an audit manager or provide an audit trail.
- **Local reporting.** Specific security-relevant events and violations will follow reporting procedures to the ISSO/G6/S6.
- **Remote reporting**. The ISSO/G6/S6 evaluates security-relevant events and reports specified occurrences to the brigade systems integrator for evaluation and investigation, if warranted.
- **Recovery action.** The proposed brigade automation officer evaluates/investigates security breaches, coordinates recovery actions, and assists the brigade intelligence officer in preparing reports.

Table 4-1. Incident Reporting[1]

Incident	Precedence	Action	Information
Copyright Violation	Routine	user>ISSO	S2/S3/S6/SJAG
Virus Detection	Priority	user>ISSO	S2/S3/S6
Intrusion (Internal)	Immediate	user>ISSO	S2/S3/S6
Intrusion (External)	Immediate	user>ISSO	S2/S3/S6
Malicious Code	Priority	user>ISSO	S2/S3/S6
Unauthorized Monitoring	Priority	user>ISSO	S2/S3/S6/SJAG
Compromise	Priority	user>ISSO	S2/S3/S6

[1] Commanders, based on staff evaluations, will determine external brigade reporting IAW AR 380-19, and CJCSI 6510.01B.

PASSWORD CONTROL

4-82. The ISSO or designated representative oversees generation, issuance, and control of all passwords. Password issuance is performed IAW AR 380-19. Basic password guidelines are–

- Users will not have any control over choosing their passwords.
- After generation, password handling and storage are at levels of the most sensitive data contained in the system. Knowledge of individual passwords will be limited to a minimum number of people and not shared. Password issuance is only to users authorized to access the system.
- At the time of password issuance, all users receive a briefing on–
  - Exclusiveness, classification, and uniqueness of each password.
  - Safeguard measures required for classified and unclassified passwords.
  - Prohibitions against disclosure to unauthorized personnel to include personnel assigned to the same project and hold identical clearances.
  - Requirement to inform an ISSO immediately of password disclosure or misuse or other potentially dangerous practices.
  - Issuance of the same password only once. Passwords will be retired when the time limit has expired or the user has transferred to other duties, reassigned, retired, discharged, or otherwise separated from the duties or the function for which the password was required. Passwords, as unique identifiers of individual authority and privileges, are strictly for use by one user.

- All passwords on classified systems change at least quarterly. Passwords on non-sensitive and sensitive but unclassified (SBU) systems change at least semi-annually.
- Passwords need protection against unauthorized observation on terminals and video displays.

COMMUNICATIONS SECURITY

4-83. COMSEC policies establish requirements designed to deny unauthorized persons access to classified or SBU information during electrical transmission from the sender to the receiver. They establish requirements designed to prevent the disclosure of valuable information from other aspects of communications (for example, traffic flow and message analysis) and to enhance the authentication of communications. The G6/S6/S3 is responsible for COMSEC; however, the NSA controls COMSEC through account holders on the global level. See AR 380-40 and TB 380-41 for more information concerning COMSEC.

EMERGENCY PROCEDURES

4-84. Some cases require emergency procedures to protect our nation's networks. Local SOPs generally explain these emergencies. The procedures are carried out only if the commander directs it or under extreme emergencies. They are–

- Zeroize COMSEC devices.
- Purge systems.
- Destruct classified systems **only when capture is imminent**.
- Notify activities as required to enable a proper response.